



Asset Management Standard

Document Name: Asset Management

Effective Date: October 15th, 2018

Document ID: IS.004

Last Revised Date: October 4th, 2018

Table of contents

1. Purpose.....	2
2. Authority	2
3. Scope	2
4. Responsibility	2
5. Compliance	2
6. Standard Statements.....	3
6.1. Information Asset Management.....	3
6.2. Information Classification.....	4
6.3. Information Labeling and Handling.....	5
6.4. Information Disposal	5
6.5. Information Protection Requirements.....	7
6.6. Information System Classification	7
6.7. Endpoint Security	8
6.8. Mobile Device Management.....	9
7. Control Mapping.....	11
8. Related Documents	11
9. Document Change Control.....	12

1. PURPOSE

- 1.1. The purpose of this **standard** is to document the requirements and key security considerations to enable the ongoing ownership and effective management of Commonwealth's **information assets**.

2. AUTHORITY

- 2.1. M.G.L. Ch. 7d provides that "Notwithstanding any general or special law, rule, regulation, executive order, policy or procedure to the contrary, all executive department agencies shall, and other state agencies may, adhere to the policies, procedures and objectives established by the executive office of technology services and security with respect to activities concerning information technology."

3. SCOPE

- 3.1. This document applies to the use of information, information systems, electronic and computing devices, applications, and network resources used to conduct business on behalf of the Commonwealth. The document applies to the Executive Department including all executive offices, and all boards, commissions, agencies, departments, divisions, councils, and bureaus. Other Commonwealth entities that voluntarily use or participate in services provided by the Executive Office of Technology Services and Security, such as mass.gov, must agree to comply with this document, with respect to those services, as a condition of use. Executive Department agencies and offices are required to implement procedures that ensure their **personnel** comply with the requirements herein to safeguard information

4. RESPONSIBILITY

- 4.1. The Enterprise Security Office is responsible for the development and ongoing maintenance of this **standard**.
- 4.2. The Enterprise Security Office is responsible for this **standard** and may enlist other departments to assist in the maintaining and monitoring compliance with this **standard**.
- 4.3. Any inquiries or comments regarding this **standard** shall be submitted to the Enterprise Security Office by sending an email to [EOTSS-DL-Security Office](#).
- 4.4. Additional **information** regarding this **standard** and its related standards may be found at <https://www.mass.gov/cybersecurity/policies>.

5. COMPLIANCE

- 5.1. Compliance with this document is mandatory for the Executive Department including all executive offices, boards, commissions, agencies, departments, divisions, councils, and bureaus. Violations are subject to disciplinary action in accordance to applicable employment and collective bargaining agreements, up to and including the termination of their employment and/or assignment with the Commonwealth.

Exceptions to any part of this document must be requested via email to the Security Office ([EOTSS-DL-Security Office](#)). A policy exception may be granted only if the benefits of the exception outweigh the increased risks, as determined by the Commonwealth CISO.

6. STANDARD STATEMENTS

6.1. Information Asset Management

All **information assets** shall be accounted for and have an assigned owner.

6.1.1. Inventory of **information assets**

Commonwealth agencies shall identify all **information assets** (i.e., physical and logical) and document the importance of these assets. The asset inventory should include all information necessary in order to effectively manage the **information asset** throughout its life cycle from creation/receipt through disposal. At a minimum, the following attributes shall be recorded (where applicable):

- 6.1.1.1. **Information system** type (e.g., server, router, smartphone)
- 6.1.1.2. Manufacturer (e.g., Cisco, Dell, Apple)
- 6.1.1.3. Model and/or version number
- 6.1.1.4. Asset tag, serial number or some other unique identifier
- 6.1.1.5. IP address (if applicable)
- 6.1.1.6. **Information Owner** (business and technical)
- 6.1.1.7. Classification level
- 6.1.1.8. Business criticality
- 6.1.1.9. Physical location (office building, room, city and state) and details of the virtual environment (if applicable)
- 6.1.1.10. License information and details regarding ownership, expiration and maintenance (if applicable)
- 6.1.1.11. End-of-support/end-of-life date and considerations (if applicable)

6.1.2. Ownership of **information assets**

Information Owners shall be identified for all **information assets**. The implementation of specific controls may be delegated by the **Information Owner**, as appropriate, but the owner remains responsible for the management and security of the **information asset**. Specifically, the **Information Owner** shall:

- 6.1.2.1. Ensure that the **information asset** is accurately inventoried and classified.
- 6.1.2.2. Ensure that the **information asset** has appropriate access restrictions.
- 6.1.2.3. Perform periodic reviews to verify appropriate access; review frequency shall be dictated by the application classification level.
- 6.1.2.4. Manage risk to the information asset, including mitigating the risks associated with operating at end-of-support/end-of-life (if applicable).

6.1.3. Acceptable use of assets

- 6.1.3.1. All Commonwealth Executive agencies and offices with **personnel** that access to **information assets** owned or managed by the Commonwealth must be aware of their associated permissions and restrictions.

6.2. Information Classification

The classification or sensitivity level of all information must be established to ensure that appropriate measures are taken to protect the information commensurate with its value to the organization and the legal restrictions on its dissemination. The **Information Custodian** is responsible for assigning the appropriate classification level.

- 6.2.1. **Confidential** — organization or customer information that if inappropriately accessed or disclosed could cause adverse financial, legal, regulatory or reputational damage to the Commonwealth, its constituents, customers and business partners.

Except as required by law, **confidential** information must be access restricted to a narrow subset of **personnel** who have a business need to access the information. Examples include:

- 6.2.1.1. Personally identifiable information (PII)
- 6.2.1.2. Regulated information (Health Insurance Portability and Accountability Act (HIPAA), Payment Card Industry (PCI), Federal Tax Information (FTI) and other types of information)
- 6.2.1.3. Employee performance and appraisal documentation
- 6.2.1.4. Internal, external and regulatory audit reports.
- 6.2.1.5. Information on the Commonwealth's security posture (e.g., firewall setting information, security configurations, vulnerability test reports, breach reports)
- 6.2.1.6. Passwords or any form of security **key**

- 6.2.2. **Internal Use** — information that has NOT been expressly authorized for public release but that has not been classified as **confidential**. The disclosure of **Internal Use** information is unlikely to have a material financial, legal, regulatory or reputational impact on the Commonwealth, its constituents, customers and business partners. Examples include:

- 6.2.2.1. Organization charts and **personnel** directories
- 6.2.2.2. Internal policies and documentation
- 6.2.2.3. **Personnel** awareness and training collateral

- 6.2.3. **Public** — information that has been expressly approved for public release. Examples include:

- 6.2.3.1. Press releases
- 6.2.3.2. Information on public facing websites (e.g., Mass.gov)

6.2.3.3. Promotional materials for Commonwealth constituent services (e.g., Medicaid enrollment)

6.2.3.4. Advertising of open positions and roles

6.3. Information Labeling and Handling

6.3.1. Procedures for the handling and labeling of information, both in electronic and physical formats, shall be defined and also account for legal and regulatory obligations.

6.3.2. Data loss prevention (DLP) technologies approved or managed by the Enterprise Security Office shall be implemented to monitor data-at-rest, data-in-transit and data-in-use.

6.3.3. Information must be protected in line with its assigned level of classification. Classification levels must be reviewed and updated at least annually.

6.3.4.1. Limit direct access to **confidential** customer information (e.g., SSN) whenever possible. Access to information must be limited to those with a need to know.

6.3.4.2. Use disclaimer statements when transferring information to internal and external parties.

6.3.4.3. The sending of Commonwealth **confidential** information to personal email addresses (e.g., Gmail or Yahoo Mail) is prohibited.

6.3.4.4. Use encryption to protect data at rest and in transit, commensurate to its classification level (See *Approved Cryptographic Techniques in the Cryptographic Management Standard*).

6.3.4. Information available in a physical format (e.g., paper) shall be labeled accordingly.

6.3.5. Protect media containing Commonwealth information against unauthorized access, misuse or corruption during transportation.

6.3.5.1 Verify the identity of couriers.

6.3.5.2 Use only authorized couriers to send **confidential** information.

6.3.5.3 Refrain from marking exterior packaging of **confidential** information with the classification level. Package sufficiently to protect the contents from physical damage.

6.3.5.4 Maintain an audit **log** of the content of the media, including the information protection applied and transportation logistics.

6.3.6. Commonwealth Executive Offices and Agencies shall by default restrict removable media use for personnel (see *Endpoint Protection in Asset Management Standard*). Removable media use shall be granted on an exception basis when there is a compelling organizational need.

6.4. Information Disposal

Establish procedures for the secure disposal and sanitization of media to minimize the risk of **confidential** information leakage.

6.4.1 Log the disposal of confidential information to maintain an audit trail.

6.4.2 Verify that the **information assets** containing any **confidential** information have been removed or securely overwritten prior to **disposal** or reuse.

6.4.2.1 Render media unusable (e.g., degaussing), unreadable or indecipherable prior to disposal.

6.4.2.2 Use acceptable industry standard (e.g., 7-pass overwrite) for information erasure to ensure information is unrecoverable.

6.4.2.3 Use a third-party service that specializes in information or media disposal.

6.4.2.4 Identify and securely delete stored information that exceeds defined retention periods on a quarterly basis.

6.4.2.5 Hard copies of information shall only be generated when necessary. Excess copies must be disposed of securely (e.g., shredding).

6.4.2.6 Regulatory compliance requirements may supersede this standard.

6.5. Information Protection Requirements

The following table summarizes the information protection requirements for Commonwealth information.





Security Considerations	Public	Internal Use	Confidential
Impact of unauthorized disclosure	No harm.	Limited harm.	Significant harm.
Access restrictions	None.	Access normally restricted to employees and approved non-employees for business purposes only.	Access granted only to authorized individuals.
Encryption	None required.	None required.	Commonwealth-approved encryption required (see Approved Cryptographic Techniques in the Cryptographic Management Standard).
Physical labeling (paper, magnetic media, CD/DVD/USB or tape label)	None required.	Information classification label must be visible. All magnetic media assets must be sent in lockable containers with a label affixed across the opening of the container.	Information classification label must be visible. All magnetic media assets must be sent in lockable containers. The label should not be affixed on outside of shipping container.
Electronic labeling (digital file, email or webpage)	None required.	E-mail: non-disclosure disclaimer must be visible.	E-mail: information must be labeled and encrypted.
Physical disposal (paper, tape or hard drives)	None required.	After applicable electronic disposal, secure onsite or off-site physical disposal using Commonwealth-approved methods.	After applicable electronic disposal, secure onsite disposal using Commonwealth-approved methods. Paper – Shred or use secure disposal bins. Electronic media — render unreadable or unrecoverable, depending on the use case. Disposal audit trail required.
Electronic disposal (Digital file)	None required.	Removal of the directory entry for the file.	Removal of the directory entry for the file. File space should be over-written using industry standard where possible.

6.6. Information System Classification

To promote a consistent approach to risk management, business continuity and disaster recovery, etc. process, all **information systems** shall be classified. **Information Owners** are responsible for determining the **information system** classification of their **information system**.

- 6.6.1 The classification of an **information system** shall be based on its most critical component (e.g., where information is transmitted, processed or stored).
- 6.6.2 Commonwealth agencies must conduct a business impact analysis or a risk assessment to determine **information system** classifications for its **information assets**.
- 6.6.3 **Information system** classification must be reviewed at least annually and whenever a significant system change occurs.

6.6.4 Classify all **information systems** as follows:

Classification level(s)	Description
	Critical <ul style="list-style-type: none"> • Information assets subject to legal and/or regulatory requirements if breached (e.g., HIPAA, PCI) • Critical core network infrastructure, including perimeter firewalls, routers, switches, domain name server (DNS) and cloud services • Systems that generate or manage in excess of \$1m or more per annum for the Commonwealth (e.g., HIX, MMIS) • Systems involved in the transmission or processing of financial information
	High <ul style="list-style-type: none"> • High-value assets that store, process or transmit confidential information • Core business support systems (e.g., email) • Externally facing systems that process or handle confidential information • Systems that impact payroll or similar internal processes • End-of-life information systems no longer supported by a vendor and without a risk exception on file • Confidential information
	Medium <ul style="list-style-type: none"> • Non-core business support systems, including externally facing systems that do not process confidential information • Internal Use information
	Low <ul style="list-style-type: none"> • Development, test and quality assurance environments or user workstations • Public information

6.7. Endpoint Security

6.7.1 Endpoint security controls to protect against malicious software, including viruses and malware, shall be implemented.

6.7.1.1 Implement antivirus solutions on all endpoints.

6.7.1.2 Implement endpoint detection and response (EDR) solutions on high-risk **information systems** (including endpoints) that store confidential data persistently.

6.7.1.3 Configure antivirus and/or EDR solutions to detect, remove and protect against known types of malicious software.

6.7.1.4 Configure antivirus and/or EDR solutions so that they cannot be circumvented, disabled or removed from an endpoint by an end user.

6.7.1.5 Update antivirus definitions in accordance with their severity rating (*Vulnerability Management Standard*). Signature definitions must be centrally managed (e.g., ePolicy Orchestrator) and pushed to endpoints. End users must not be able to prevent updates to their Commonwealth-issued endpoint.

6.7.1.6 Retain audit logs for antivirus and EDR solutions for at least one year with a minimum of three (3) months readily available for analysis (see *Logging and Event Monitoring Standard*).

6.7.1.7 Integrate antivirus and EDR solutions with the enterprise SIEM, where technically feasible.

6.7.1.8 Full-disk encryption must be configured for all laptops. Desktops that store **confidential** information on a persistent basis must implement full-disk encryption.

- 6.7.1.8.1 Encryption keys must be centrally managed. Mechanisms to recover encryption keys in the case of loss shall be available and tested.
- 6.7.2 Implement host-based firewall solutions for **information systems** with direct connectivity to the Internet (e.g., laptops used by **personnel** at home or on public Wi-Fi), which are used to access the organization's network.
- 6.7.3 Implement host-based firewalls for end of life (EOL) **information systems**.
- 6.7.4 Implement host-based intrusion prevention systems (IPS) on high-risk systems.
- 6.7.5 Implement controls to protect endpoints from virus and malware that can be introduced via removable media (e.g., USB storage media).
 - 6.7.5.1 Auto scan removable media for virus and malware prior to use.
 - 6.7.5.2 Disable functionality that allows auto-run upon insertion of removable media.
 - 6.7.5.3 Force encryption on removable media prior to allowing information transfer to and from the media.
- 6.7.6 Implement technical controls to restrict the installation of unauthorized software on Commonwealth-owned or managed endpoints.
- 6.7.7 Restrict the use of local administrator privileges on endpoints to those individuals with a business need (e.g., help desk or designated security administrators).
 - 6.7.7.1 An up-to-date inventory of users with persistent access to administrative privileges must be maintained and reported to the Commonwealth CISO on a quarterly basis.
- 6.7.8 Perform a full antivirus and anti-malware scan on endpoints, at a minimum, monthly.
- 6.7.9 Third parties that require a connection to the Commonwealth family of networks must have up-to-date antivirus and antimalware solutions installed.

6.8. Mobile Device Management

The Commonwealth shall implement a mobile device management (MDM) solution approved and maintained by the Enterprise Security Office to manage mobile devices in its environment.

- 6.8.1 The MDM solution shall support, at a minimum, the following functionalities:
 - 6.8.1.1 Provides the highest coverage of mobile devices and operating systems
 - 6.8.1.2 Inventory management (i.e., self-enrollment, directory integration, enforcement of acceptable use policy, remote wipe, backup and restore)
 - 6.8.1.3 Device policy management (i.e., centralized enforcement of policy, group/location policies, compliance checks)
 - 6.8.1.4 Security management (i.e., information and device encryption, information segmentation, logging and monitoring, password/PIN management, jailbreak detection)

6.8.1.5 Monitoring and reporting (i.e., configurable dashboard, device tracking, canned/custom reporting)

Controls shall be implemented to prevent unauthorized disclosure of information on mobile devices (e.g., mobile phones and tablets). At a minimum, the following shall be adhered to:

6.8.2 Users must obtain authorization to use a personal mobile device to directly access Commonwealth information.

6.8.2.1 Users that voluntarily choose to use their personal mobile device for Commonwealth business must sign off that they understand the risk of using a mobile device and adhere to Commonwealth policies and standards.

6.8.2.2 Sign off that he/she understands and accepts risks associated with using a mobile device that is owned or managed by the Commonwealth, including inclusion in the mobile inventory, installation of an MDM solution, enforcement of password policy, authorization to review and retrieve phone information and remote wipe.

6.8.3 Create an inventory of all mobile devices (Commonwealth-owned and personal) that connect to the Commonwealth family of networks. The inventory shall be reviewed at least annually and include ownership information and device specifications (e.g., manufacturer, model, OS).

6.8.4 Personal mobile devices that directly connect to the Commonwealth family of networks or that have direct access to Commonwealth's **confidential information** shall connect via VPN and an inventory of devices authorized to connect must be actively maintained (see *Remote Access in the Network and Communication Security Standard* and *Information Asset Management in the Asset Management Standard*).

6.8.5 Commonwealth-owned information-at-rest on mobile devices shall be encrypted with an approved software encryption solution (see *Approved Cryptographic Techniques in the Cryptographic Management Standard*).

6.8.6 Enforce password requirements for mobile devices through technical means as outlined in *Password Management in the Access Management Standard*.

6.8.7 Restrict mobile device users from making modifications of any kind to Commonwealth-owned or installed hardware and software on the mobile device.

6.8.8 Mobile devices, regardless of ownership, housing Commonwealth information shall be securely decommissioned, when no longer needed for business or legal reasons.

6.8.9 Commonwealth agencies must ensure mobile device users are aware of the risks involved with mobile computing and the types of information that can and cannot be stored on such devices, through regular security awareness training.

7. CONTROL MAPPING

Section	NIST SP800-53 R4 (1)	CIS 20 v6	NIST CSF
6.1 Information Asset Management	CM-8	CSC 1	ID.AM-1
	CM-9	CSC 3	PR.IP-1
	PM-5	-	-
	PL-4	-	-
		CSC 2	ID.AM-2
6.2 Information Classification	RA-2	-	ID.AM-5
6.3 Information Labeling and Handling	AC-16	CSC 5	PR.AC-4
	MP-2	CSC 8	PR.PT-2
	MP-3	-	-
	SC-16	-	-
6.4 Information Disposal	SI-12	-	-
		-	PR.IP-6
	MP-6	CSC 1	PR.DS-3
6.5 Information Protection Requirements	AC-22	-	-
	AC-3	CSC 5	PR.AC-4
	MP-Family	-	-
	SC-28	CSC 14	PR.DS-1
	SI-12	-	-
6.6 Information System Classification	RA-2	-	ID.AM-5
6.7 Endpoint Security	PE-16	CSC 1	PR.DS-3
	SI-12	-	-
	MP Family	-	-
	PE-2	-	PR.AC-2
	PE-3	-	PR.AC-2
	PE-6	-	PR.AC-2
	PE-7	-	-
	PE-8	-	-
	PE-18	-	PR.IP-5
	AU-1	-	ID.GV-1
	AU-2	CSC 6	PR.PT-1
	AU-3	CSC 6	PR.PT-1
	AU-4	-	PR.DS-4
	AU-5	CSC 6	PR.PT-1
	AU-6	CSC 6	PR.PT-1
	AU-7	CSC 6	PR.PT-1
	AU-9	CSC 6	PR.PT-1
	AU-11	CSC 6	PR.PT-1
	AU-12	CSC 6	PR.PT-1
	AU-14	CSC 6	PR.PT-1
	SI-4	CSC 4	ID.RA-1
		-	DE.DP Family
6.8 Mobile Device Management	CM-8	CSC 1	ID.AM-1
	AC-1	-	ID.GV-1
	AC-17	CSC 12	PR.AC-3
	AC-18	CSC 11	PR.PT-4
	AC-19	CSC 12	PR.AC-3
	PL-4	-	-
	PS-6	CSC 13	PR.DS-5
	AC-24	-	-

8. RELATED DOCUMENTS

Document	Effective date

9. DOCUMENT CHANGE CONTROL

Version No.	Revised by	Effective date	Description of changes
0.9	Jim Cusson	10/01/2017	Corrections and formatting.
0.95	John Merto	12/22/2017	Wording
0.96	Sean Vinck	5/7/2018	Corrections and formatting.
0.97	Andrew Rudder	5/31/2018	Corrections and Formatting.
0.98	Anthony O'Neill	05/31/2018	Corrections and Formatting.
1.0	Dennis McDermitt	6/1/2018	Final Pre-publication Review
1.0	Andrew Rudder	10/4/2018	Approved for Publication by: John Merto

The owner of this document is the Commonwealth CISO (or designee). It is the responsibility of the document owner to maintain, update and communicate the content of this document. Questions or suggestions for improvement should be submitted to the document owner.

9.1 Annual Review

This *Asset Management Standard* should be reviewed and updated by the document owner on an annual basis or when significant policy or procedure changes necessitate an amendment.